(12) UK Patent Application (19) GB (11) 2 278 518 (13) A

(43) Date of A Publication 30.11.1994

(21) Application No 9309911.7

(22) Date of Filing 14.05.1993

(51) INT CL[5]
H04L 9/16 9/32

(52) UK CL (Edition M)
H4P PDCSA PDCSX

(56) Documents Cited
EP 0393806 A2 EP 0257585 A2 EP 0197392 A2
EP 0064779 A2 US 4567600 A

(58) Field of Search
UK CL (Edition M) H4P PDCSA PDCSC PDCSP PDCSX
INT CL[5] H04L 9/14 9/16 9/30 9/32
ONLINE DATABASES : WPI

(71) Applicant(s)
Trafford Limited

(Incorporated in the United Kingdom)

66 Newland Street, WITHAM, Essex, CM8 1AH, United Kingdom

(72) Inventor(s)
Douglas Stewart Miller

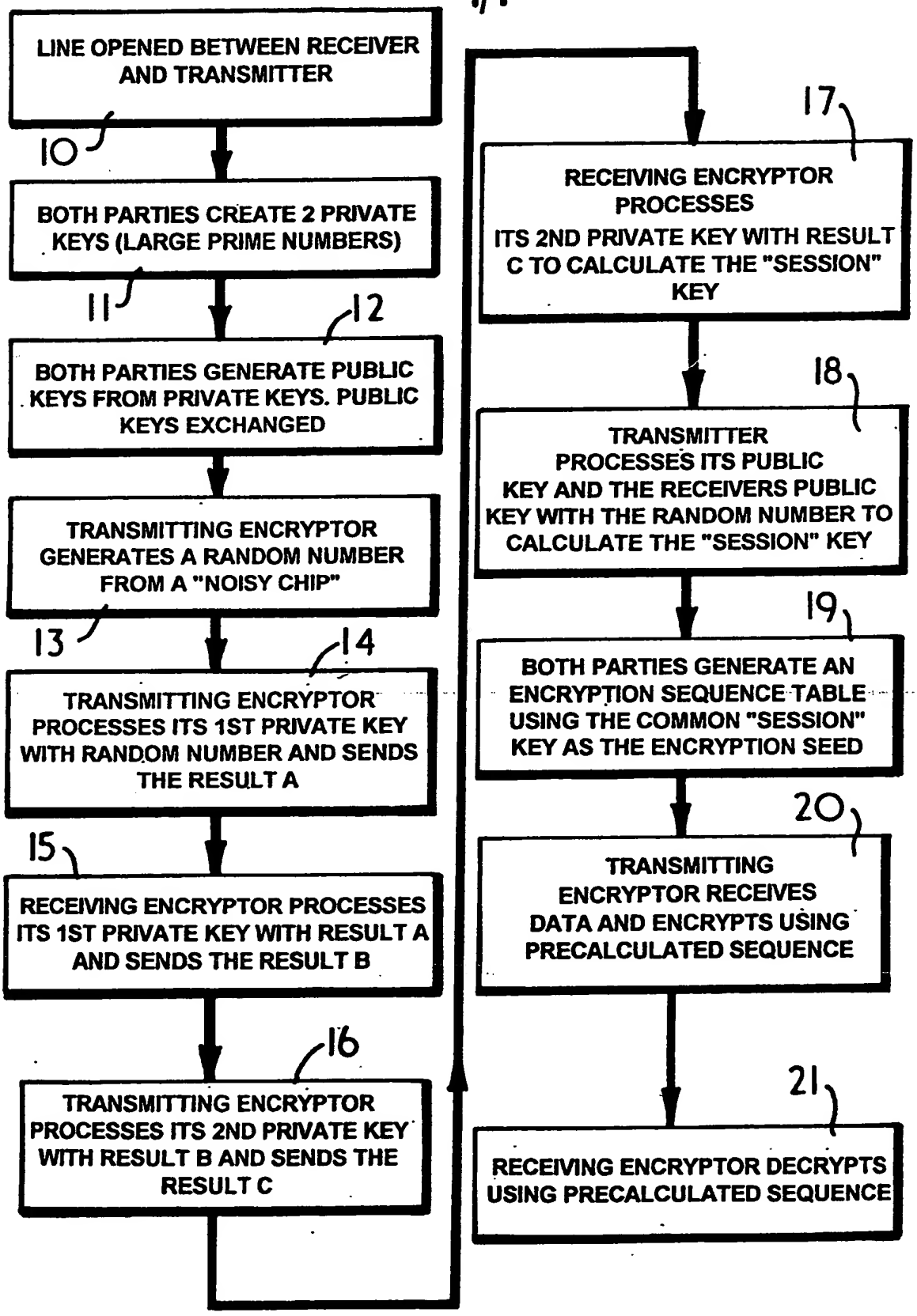
(74) Agent and/or Address for Service
Sanderson & Co
34 East Stockwell Street, COLCHESTER, Essex, CO1 1ST, United Kingdom

(54) Encrypted data transfer

(57) A method of and apparatus for encrypted data transfer between a transmitter and a receiver (e.g. fax stations) utilises a series of steps which result in the possibility of transferring a message so encrypted that even unauthorised tapping of the transfer will not enable discovery of the keys used for encryption. Both the transmitter and the receiver have first and second private keys which keys are used to generate respective public keys which are then exchanged. A new (to the transmitter) random number is generated in the transmitter and processed with the transmitter first private key to yield a first result which is passed to the receiver. The receiver processes that result with its first private key to yield a second result which is passed back to the transmitter. That second result is processed with the transmitter second private key to yield a third result which is passed to the receiver. That third result is processed with the receiver second private key to yield a session key. The random number is processed in the transmitter with both the transmitter and receiver public keys to yield the session key. Thereafter, with both the transmitter and the receiver in possession of the session key, an exchange of data encrypted with the session key may take place.

Generation of the public keys from the private keys involves a predetermined prime number pre-set in the transmitter or receiver during its manufacture.

GB 2 278 518 A


LINE OPENED BETWEEN RECEIVER AND TRANSMITTER
10
BOTH PARTIES CREATE 2 PRIVATE KEYS (LARGE PRIME NUMBERS)
11
12
BOTH PARTIES GENERATE PUBLIC KEYS FROM PRIVATE KEYS. PUBLIC KEYS EXCHANGED
TRANSMITTING ENCRYPTOR GENERATES A RANDOM NUMBER FROM A "NOISY CHIP"
13
14
TRANSMITTING ENCRYPTOR PROCESSES ITS 1ST PRIVATE KEY WITH RANDOM NUMBER AND SENDS THE RESULT A
15
RECEIVING ENCRYPTOR PROCESSES ITS 1ST PRIVATE KEY WITH RESULT A AND SENDS THE RESULT B
16
TRANSMITTING ENCRYPTOR PROCESSES ITS 2ND PRIVATE KEY WITH RESULT B AND SENDS THE RESULT C
17
RECEIVING ENCRYPTOR PROCESSES ITS 2ND PRIVATE KEY WITH RESULT C TO CALCULATE THE "SESSION" KEY
18
TRANSMITTER PROCESSES ITS PUBLIC KEY AND THE RECEIVERS PUBLIC KEY WITH THE RANDOM NUMBER TO CALCULATE THE "SESSION" KEY
19
BOTH PARTIES GENERATE AN ENCRYPTION SEQUENCE TABLE USING THE COMMON "SESSION" KEY AS THE ENCRYPTION SEED
20
TRANSMITTING ENCRYPTOR RECEIVES DATA AND ENCRYPTS USING PRECALCULATED SEQUENCE
21
RECEIVING ENCRYPTOR DECRYPTS USING PRECALCULATED SEQUENCE

ENCRYPTED DATA TRANSFER

This invention relates to a method of and apparatus for establishing an encrypted data transfer link between a transmitter and a receiver, suitable for use, for example, with facsimile transmissions, amongst other uses.

Data of a very wide variety of kinds is frequently transmitted over radio or land-line links. It may be desirable, for commercial or other reasons, to maintain secret such data as is being transmitted. Conveniently, this is achieved by encrypting the data prior to its transmission over a radio or land-line link, in order that the data, if intercepted either accidentally or deliberately during its transmission, will be unintelligible to the interceptor.

In order to allow encrypted and transmitted data to be decrypted upon its reception by an authorised recipient, that recipient must be in possession of the key which was used to encrypt the data at the transmitter. Complex schemes for key management have been evolved to minimise the likelihood of a key falling into unauthorised hands, but generally speaking these management systems require at least one key physically to be transferred to the data recipient before the transmission of encrypted data, in order that the key might be used to decrypt the encrypted

data, upon its reception.

Though it would be desirable from the convenience point of view, heretofore it has generally been accepted that the transmission of a key over a data transmission link does not afford sufficient security, since the interception of the transmitted key will enable the subsequent unauthorised decryption of an encrypted transmission. If the key is encrypted before its transmission, there still has to be a key transfer to the recipient, in order that he might decrypt the received key and the same problems arise concerning that key as have been discussed above.

It is a principal aim of the present invention to provide a method of establishing an encrypted data transfer link, where the key used for encryption and decryption is transmitted over the data transfer link, in such a way that the key itself cannot be determined from an interception of the transmitted data over the data transmission link, and which does not require any other physical key transfer between the transmitter and the receiver.

Accordingly, one aspect of the present invention provides a method of establishing an encrypted data transfer link between a transmitter and a receiver, comprising the steps of: separately establishing in each of the transmitter and the receiver first and second private keys; in each of the transmitter and the

receiver generating a public key from the respective first and second private keys; exchanging the public keys over the data transfer link; establishing a random number in the transmitter; processing the random number with the transmitter first private key to yield a first result and then passing said first result to the receiver; processing in the receiver said first result with the receiver first private key to yield a second result and then passing said second result to the transmitter; processing in the transmitter said second result with the transmitter second private key to yield a third result and then passing said third result to the receiver; processing in the receiver said third result with the receiver second private key to yield a session key; processing in the transmitter said random number with the transmitter public key and the receiver public key to yield said session key; utilising said session key in the transmitter to encrypt data subsequently passed to the receiver and utilising said session key in the receiver to decrypt encrypted data received from the transmitter.

In the method of the present invention, the key used for encrypting and decrypting the principal data to be transmitted over the link is itself not transmitted over that link. Instead, only processed forms of that key are transmitted, and in such a way that insufficient data is transmitted over the data

transfer link to enable the calculation of the key itself, merely by intercepting the transmissions. However, at the completion of the establishment of the encrypted data transfer link, both the transmitter and the receiver are in possession of the same session key to be used for the transmission of encrypted data, which thus may be transmitted with a relatively high degree of security.

During the initial stages of the setting up of the encrypted data link, first and second private keys are established in both the transmitter and the receiver. Preferably, both private keys are relatively large prime numbers, and fresh first and second private keys are established each time an encrypted data link is to be set up between a transmitter and a receiver. To enhance security, the established private keys are advantageously not selected to be the same as any private keys which have previously been used by the establishing transmitter, or receiver, as appropriate. Conveniently, the last-used first and second private keys are stored, and then the new keys to be established are selected to be higher than the stored, last-used keys; in this way, it is relatively easy to ensure that neither the first nor second private key has been used before, without the need to store more than two previously-used keys.

The public key may be generated by multiplying the

first and second private keys together, and then processing the result with a pre-determined prime number, and preferably by performing modulo arithmetic on said result, using the prime number as the divisor. The predetermined prime number may be pre-set in the transmitter or receiver, as appropriate, during its manufacture. The equipment manufacturer may ensure that each transmitter or receiver produced by him has a different pre-set prime number permanently established therein, for the purpose of this processing.

Though the random number to be established in the transmitter could be a pseudo-random number generated by a mathematical sequence, preferably said random number is a truly random number, of the same order of magnitude as each of the private keys. For example, the random number could be generated by a "noisy" semiconductor junction.

The processing of the random number to yield said first result may include the step of raising the first private key to the power of the random number, and then performing modulo arithmetic on the result. Such modulo arithmetic preferably is performed using the same pre-determined prime number as the base, as is employed to generate the public key.

Subsequent processing, to obtain said second and third results, advantageously is performed in precisely the same manner to the processing of the random number,

to obtain said first result, but by operating on said first result and said second result, respectively. Thus, all of the modulo arithmetic steps are performed using the pre-determined prime number which is advantageously unique to the transmitter or receiver, as appropriate.

Once the session key has been established in both the transmitter and the receiver, it may be used in any known way, to perform the encryption and decryption of data transmitted between the two. For example, the session key may be used to seed look-up tables for the data to be transmitted and for the data to be decrypted once received; such techniques are well understood in the art and will not be described in further detail here.

Security of the system described above may be enhanced by increasing the size of the first and second private keys, the public key, the random number and the pre-determined prime number. For many purposes, sufficient security may be achieved with eight-digit numbers, but by increasing the size of each of those numbers, the security of the system may be increased. It is envisaged that for very secure data transmission links, relatively large numbers may be chosen - and perhaps as large as forty-digit numbers.

According to a second aspect of this invention, there is provided a transmitter or a receiver

configured to permit the establishment of an encrypted data transfer link therebetween in accordance with the method of this invention as described above, there being in the transmitter or the receiver means for establishing first and second private keys, means to establish a random number, means storing a pre-set prime number, and processing means to operate on the first and second private keys, an established random number and the pre-set prime number and also on numbers transferred over the data link from a corresponding receiver or transmitter as appropriate, whereby in use of a transmitter and receiver both may come in possession of the same session key for an encrypted data transfer solely by the transmission of data over the link but without the transmission of the session key or an encrypted form of that key.

By way of example only, one specific example of a data transfer method according to the present invention will now be described in detail, reference being made to the accompanying drawing, which shows in block form the various steps adopted to establish the secure transfer of data from a transmitter to a receiver.

In general, it is envisaged that data will be transferred from one station to an essentially identical station; such stations may for example be fax (facsimile) machines furnished with the appropriate hardware and software to enable the secure transfer of

data from one machine to the other, by a method falling within the scope of this invention. As the stations are essentially identical, the secure transfer of data may take place in either direction, with either station serving as the transmitter, and the other station as the receiver, for the time being.

Both the transmitter and the receiver are furnished with a respective encryptor/decrypter (referred to hereinafter just as an "encryptor"), in effect interposed between the data generator (a computer or a conventional fax machine) and a modem normally associated with the computer or fax machine, to allow the transmission of digital data over a data link. Each encryptor has permanently established therein, by the manufacturer of the encryptor, a pre-set prime number. Moreover, the manufacturer of the encryptors ensures that each encryptor manufactured to a particular specification and able to operate with a similar encryptor has a different pre-set prime number permanently established therein, further to enhance security.

The method could be used over any kind of data transmission link between the two stations. For example, there may be a dedicated land line between the two stations, a radio or microwave link, a fibre optic link or any other appropriate data link. However, for many purposes, and particularly when the transmitter

and receiver are fax machines, conventional telephone circuits may be employed. Though such circuits are not immune to eaves-dropping, nevertheless the encryption method of the present invention allows secure data transfer.

Referring now to the drawing, the first step in preparing for the secure transfer of data from one station to another is to open a line between the transmitter and the receiver, as shown by stage 10. In the case of fax machines, this stage will comprise the transmitter machine dialling the conventional public telephone number of the receiver machine and then, when the receiver machine answers, establishing communication between the two machines, via their respective modems.

In stage 11, both the transmitter and the receiver generate first and second private keys respectively, which are relatively large prime numbers, perhaps of forty digits length each, though to reduce subsequent processing time, shorter private keys could be generated. The encryptors are arranged to ensure that the private keys generated during this stage, at the commencement of the establishment of a secure data link between a transmitter and a receiver, are previously-unused keys. For example, each encryptor may store the last generated private key and ensure that the next generated private key is always larger (but it could

always be smaller) than the last generated key.

In stage 12, both the transmitter and the receiver generate a public key, from the first and second private keys generated in stage 11. The public keys may be generated in the manner described hereinbefore, using the first and second private keys and also the pre-set prime number. Then, these public keys are exchanged over the data link. These public keys could be determined from unauthorised access to the data link, but are not useful, by themselves, in decrypting subsequent encrypted data transfer.

The transmitter, in stage 13, generates a relatively large random number, for example by using a "noisy" semi-conductor junction, in a manner known per se. This random number should be of the same order of magnitude as each of the private keys generated in stage 11.

In stage 14, the transmitter processes its first private key with the random number generated in stage 13, in the manner described hereinbefore to achieve a result A, which is then sent to the receiver. In stage 15, the receiver processes its first private key with received result A, in the manner described hereinbefore to achieve a result B, which is then sent to the transmitter. In stage 16, the transmitter processes its second private key with received result B, in the manner described hereinbefore to achieve a result C,

which is sent to the receiver. And then in stage 17, the receiver processes its second private key with received result C, in the manner described hereinbefore to calculate a session key.

The transmitter must also calculate the session key, and this is performed in stage 18. Here, the transmitter processes in the manner described hereinbefore its public key with the receiver's public key (received in stage 12) and then processes the result with the random number generated in the transmitter in stage 12, so obtaining the session key. Of course, this stage may be performed by the transmitter at any point after stage 13 has been completed, but not necessarily serially, after completion of stage 17.

The two identical session keys now possessed by both the transmitter and the receiver are used to encrypt the data to be transmitted and to decrypt the received data. Any suitable encryption technique which will be understood by those skilled in the art may be employed. For example, as shown in stage 19, the respective session keys may be used to "seed" encryption sequence tables established in the transmitter and the receiver, but other encryption techniques or algorithms may be employed.

Once the secure data link has been established, for the transmission of encrypted data using the unique

session keys, the actual transmission of data may commence. In stage 20, the encryptor itself of the transmitter receives data for example from a fax machine or from a computer and then encrypts that data using the encryption sequence table established in stage 19, before transmitting that data to the receiver. As shown in stage 21, the receiver receives the encrypted data and decrypts that data using the encryption sequence table which it too establsihed in stage 19.

It will be appreciated that using the method described in detail above to establish a secure data link between a transmitter and a receiver, the unique session key required for encryption and decryption is not transmitted over the data link, nor does that key have to be communicated between the transmitter and the receiver by some external means. Instead, both the transmitter and the receiver are able separately to establish the identical unique session key by appropriate processing of data transferred both ways between the transmitter and the receiver, but any unauthorised party monitoring the data link between the transmitter and the receiver will not be able also to calculate the session key. Moreover, security is greatly enhanced by the technique enabling the establishment of a unique session key for each data transfer session, so ensuring that even should a key

for one session of data transfer be, somehow, determined by a third party, that key will be of no use on a subsequent data transmission session.

CLAIMS

1. A method of establishing an encrypted data transfer link between a transmitter and a receiver, comprising the steps of:

separately establishing in each of the transmitter and the receiver first and second private keys;

in each of the transmitter and the receiver generating a public key from the respective first and second private keys;

exchanging the public keys over the data transfer link;

establishing a random number in the transmitter;

processing the random number with the transmitter first private key to yield a first result and then passing said first result to the receiver;

processing in the receiver said first result with the receiver first private key to yield a second result and then passing said second result to the transmitter;

processing in the transmitter said second result with the transmitter second private key to yield a third result and then passing said third result to the receiver;

processing in the receiver said third result with the receiver second private key to yield a session key;

processing in the transmitter said random number with the transmitter public key and the receiver public

key to yield said session key;

utilising said session key in the transmitter to encrypt data subsequently passed to the receiver and utilising said session key in the receiver to decrypt encrypted data received from the transmitter.

2. A method according to Claim 1, wherein the first and second private keys in both of the transmitter and the receiver are established by generating two relatively large prime numbers.

3. A method according to Claim 2, wherein each time first and second private keys are established in the transmitter and the receiver, the keys are not selected from those that have previously been used by the establishing transmitter or receiver, as appropriate.

4. A method according to Claim 3, wherein the established private keys are always higher or are always lower than those that were last established.

5. A method according to any of the preceding Claims, wherein said public key is generated by multiplying the first and second private keys and then processing the result with a pre-determined prime number.

6. A method according to Claim 5, wherein said processing comprises performing modulo arithmetic on said result.

7. A method according to any of the preceding Claims, wherein said random number is a truly random

number of the same order of magnitude as each of the private keys.

8. A method according to any of the preceding Claims, wherein the processing of the random number to yield said first result includes the step of raising the first private key to the power of the random number and then performing modulo arithmetic on the result.

9. A method according to Claim 5 and 8, wherein the modulo arithmetic is performed using the same pre-determined prime number as is employed to generate the public key.

10. A method according to any of the preceding Claims, wherein the processing to obtain said second and third results is performed in a similar manner to the processing of the random number to obtain said first result, but by operating on said first result and said second result, respectively.

11. A method substantially as hereinbefore described with to the accompanying drawings.

12. A transmitter or a receiver configured to permit the establishment of an encrypted data transfer link therebetween in accordance with the method any of the preceding Claims, which transmitter or receiver comprises means for establishing first and second private keys, means to establish a random number, means storing a pre-set prime number, and processing means to operate on the first and second private keys, an

established random number and the pre-set prime number and also on numbers transferred over the data link from a corresponding receiver or transmitter as appropriate, whereby in use of a transmitter and receiver both may come in possession of the same session key for an encrypted data transfer solely by the transmission of data over the link but without the transmission of the session key or an encrypted form of that key.

Patents Act 1977 Examiner's report to the Comptroller under Section 17 (The Search report)	18	Application number GB 9309911.7
Relevant Technical Fields (i) UK Cl (Ed.M) H4P (PDCSA, PDCSC, PDCSP, PDCSX) (ii) Int Cl (Ed.5) H04L 9/14, 9/16, 9/30, 9/32		Search Examiner K WILLIAMS Date of completion of Search 15 JULY 1994
Databases (see below) (i) UK Patent Office collections of GB, EP, WO and US patent specifications. (ii) ONLINE DATABASE: WPI		Documents considered relevant following a search in respect of Claims :- 1-12

Categories of documents

X:	Document indicating lack of novelty or of inventive step.	**P:**	Document published on or after the declared priority date but before the filing date of the present application.
Y:	Document indicating lack of inventive step if combined with one or more other documents of the same category.	**E:**	Patent document published on or after, but with priority date earlier than, the filing date of the present application.
A:	Document indicating technological background and/or state of the art.	**&:**	Member of the same patent family; corresponding document.

Category	Identity of document and relevant passages		Relevant to claim(s)
X	EP 0393806 A2	(TRW INC) see abstract	1,12
X	EP 0257585 A2	(NEC CORP) see whole specification	1,12
X	EP 0187392 A2	(I.B.M. CORP) see the whole specification & US 4649233	1,12
X	EP 0064779 A2	(SVENSKA PHILIPS) see pages 16-20	1,12
X	US 4567600	(OMNET ASS) see abstract	1,12

Databases:The UK Patent Office database comprises classified collections of GB, EP, WO and US patent specifications as outlined periodically in the Official Journal (Patents). The on-line databases considered for search are also listed periodically in the Official Journal (Patents).